Міністерство освіти і науки України Національний технічний університет України "Київський політехнічний інститут імені Ігоря Сікорського" Фізико-технічний інститут

КРИПТОГРАФІЯ

Комп’ютерний практикум №2

«Крипто аналіз шифру Віженера»

Виконали:

Факультет ФТІ,
група ФБ-93

Денисюк А.Г.
Товстоноженко М.С.

Київ-2021

Мета: Засвоєння методів частотного крипто аналізу. Здобуття навичок роботи та аналізу потокових шифрів гамування адитивного типу на прикладі шифру Віженера.

Завдання:

0. Уважно прочитати методичні вказівки до виконання комп'ютерного практикуму.

1. Самостійно підібрати текст для шифрування (2-3 кб) та ключі довжини r = 2, 3, 4, 5, а також довжини 10-20 знаків. Зашифрувати обраний відкритий текст шифром Віженера з цими ключами.

2. Підрахувати індекси відповідності для відкритого тексту та всіх одержаних шифр текстів і порівняти їх значення.

3. Використовуючи наведені теоретичні відомості, розшифрувати наданий шифр текст (4 варіант).

Хід роботи:

Частина 1:

1)Для шифрування було взято з інтернету текст «як забивати кальян».Також цей текст було вирішено брати не весь, а лише деякі його шматки через загальний розмір тексту.

У нашій програмі генеруємо ключі довжини 2-5 та 10-20 і за допомогою них зашифровуємо початковий текст.Оскільки текст сам по собі великий, було прийнято рішення у таблицю занести лише початкову частину тексту.

Key length	**Key**	**Ciphered text**
2	шб	Вбвишвауфлшмфаерэсъьэщшдаегакпыппужвуржм…
3	чцъ	Бцдюцыяицбцеухзжыкщсяпцэяъецииъдсйдытеив…
4	тшшд	Ьшвлтщацовшпочеучиъячршзъьгджытйкжензжп…
5	жудяа	Руожазыцыкжюаюнхшфбыллдвикюгсойбысозоунл…
10	рпхемдяшюе	Ъпяммезкъпръсдщудиаахзхификчрууэмчъеъзмр…
11	нмфъсчхрмшы	Чмюбсшэвивышиузаьетзэунпьюьцзюпжтяъххаеа…
12	гщлсшпбзьзъл	Нщхшшрйщшсъцяшшаэягвбяъолэцркэдхущимюищьл…
13	еогмбызщшюрзв	Понубыплфиртюдытссэвюрюупжрнхъдйюлжялцррб…
14	уялшжгббюнелчч	Эяхяждйуъчецуцаорииюжщюрнпвценожэхпвщьуц…
15	чгцныъчдычащьпц	Бгафыыяцчбадшогжижпцяпдюяддыбдъсняйытуйв…

16	шлфйтогтчпююпфнь	Влюртплдущюйлуълэыцдчжгхяуйэбвркпэвкнэсэ…
17	язэаеиэщцсозъеьмж	Йзззейелтыотцдйылпйшеэиабъьнщиикгшнишпуу…
18	цфщйюдгохаржьщяшыд	Афгрюеласкрсшшмзафшпюбюзлтаявфязцкйесгзфс…
19	юхвжгеехгявяплынхей	Ихмнгжнзяйвклкиьъхлщъъжжнйавсрвэвныцашма…
20	ещэнмйисцкийехъиязиг	Пщзфмкргтфифбфзчдчкюксэрфнуришлчьзийъццо…

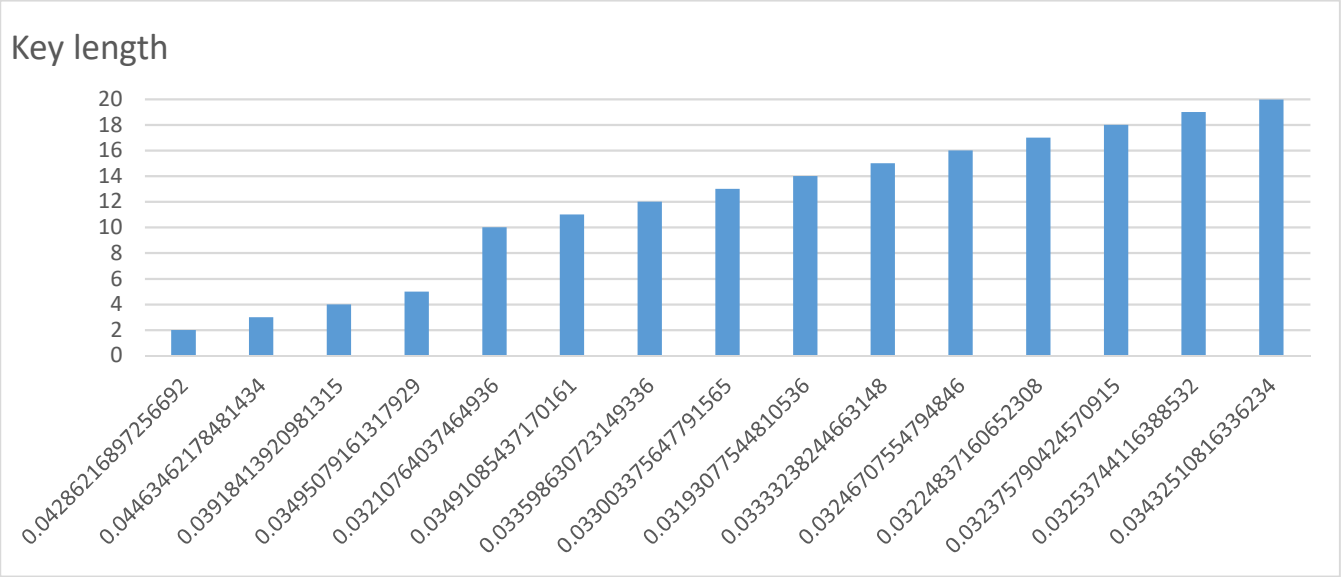
Частина 2:

2)Coincidence index початкового тексту: 0.05506394713069938

Створюємо таблицю, у яку вносимо ІВ для зашифрованого згенерованими ключами тексту.

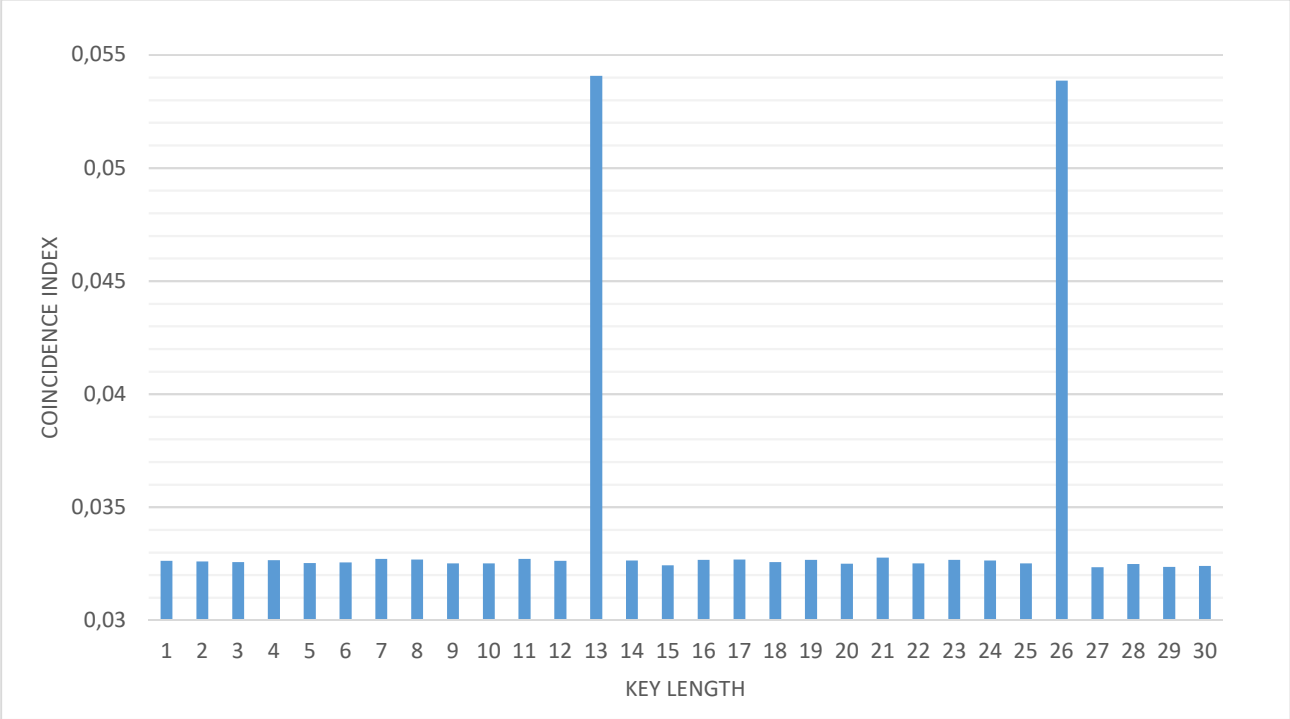
Key length	**Key**	**Coincidence index**
2	шб	0.04286216897256692
3	чцъ	0.04463462178481434
4	тшшд	0.03918413920981315
5	жудяа	0.03495079161317929
10	рпхемдяшюе	0.03210764037464936
11	нмфъсчхрмшы	0.03491085437170161
12	гщлсшпбзьзъл	0.033598630723149336
13	еогмбызщшюрзв	0.033003375647791565
14	уялшжгббюнелчч	0.03193077544810536
15	чгцныъчдычащьпц	0.03333238244663148
16	шлфйтогтчпююпфнь	0.03246707554794846
17	язэаеиэщцсозъеьмж	0.03224837160652308
18	цфщйюдгохаржьщяшыд	0.032375790424570915

19	юхвжгеехгявяплынхей	0.03253744116388532
20	ещэнмйисцкийехъиязиг	0.03432510816336234



Частина 3:

Key Length	Coincidence Index	Key Length	Coincidence Index	Key Length	Coincidence Index
1	0,03263	11	0,032714	21	0,032769
2	0,032605	12	0,032635	22	0,032516
3	0,032577	13	0,054069	23	0,032672
4	0,032651	14	0,032637	24	0,032639
5	0,032535	15	0,032436	25	0,032509
6	0,03256	16	0,032675	26	0,053855
7	0,032718	17	0,032683	27	0,032348
8	0,032692	18	0,032569	28	0,032491
9	0,032514	19	0,032665	29	0,032363
10	0,032518	20	0,032507	30	0,032398



Індекси відповідності для блоків тексту, отриманих шляхом розбиття ШТ при різній довжині ключа

Хід роботи при пошуку ключа

Написана програма відкидає значення довжини ключа, якщо відповідний їм індекс відносності схиляється до $\frac{1}{m}$ (+-0.012). Таким чином кінцевому користувачу надається два значення довжини ключа 13 і 26 а також різницю між відповідним їм індексом відносності і індексом відносності для російської мови (0.0553) - 0.0012314294 і 0.0014449378 відповідно. Програма приймає за можливе значення довжини ключа - 13, так як різниця для його ІВ і ІВ для російської мови найменша. Далі ШТ розбивається на блоки, і отримані блоки аналізуються як шифр Цезаря. Для кожного блоку знаходиться частотність символів і порівнюються з частотністю для відкритого тексту. Встановлюється відповідність між зашифрованими символами та відкритими. Таким чином генерується ключ.

Кінцевому користувачу надається змога переглянути ключі для всіх можливих допустимих довжин ключа.

При довжині ключа 13 спостерігаємо наступний такий результат:

supposable key is:громакуведьма

фвоьзтыупдыдксыогыъьжкйюыичшчфнъодтмтаангщинпафктмстлзуэешчкффьцтлзуэешчо
громакуведьмагромакуведьмагромакуведьмагромакуведьмагромакуведьмагромакув
старзииская школачырйдеевпифийинрывницфакульнентеоретичесеодипрактичесеодм

Спостерігаємо часткове розшифрування. За допомогою виділеного фрагменту можемо отримати ключ «громыковедьма», і з його допомогою розшифрувати текст.

Розшифрований текст:

старминскаяшколачародеевпифийитравницфакультеттеоретическойипрактическоймагиикаф
едрамаговпрактиковчастьперваясоциальныйукладбытинравывампирьейобщинывикачтовычт
отоимеетепротиввампировраспринкорпорациямифкурсоваяработаадептживосьмогокурсаволь
хиреднойнаучныйруководительмагистрпервойстепениархимагксанперловдевятьсотдевяност
одевятыйгодпобелорскомулетосчислениюгородстарминведениехорошийсегоднявыдалсяден
ектеплыйбезветренныйвтораядекадасеоставамесяцанеспешносочилась сквозьклепсидрусолн
ечноголетаиголосазябликовдоносившиесяизпридорожныхкустовзвенеливушахяехалась квозьи
хгнездовыеугодьякаквдольпограничнойполосыполосойбыладорогазаброшенныйпроклевыва
ющийсяпыльнойтравойкривойбольшакзябликипопеременновозмущалисьвторжениемчеловек
анабелойлошадивихчастныевладениязалихватскиетрелисменялись хриплымчириканьемптахи
суетливоперепархивалиповеточкамтревожалиствуразноцветнаякаймавокругчерныхподсыхаю
щихлужвзрывалась сотнямиистомленныхжароймотыльковраскручивалась ввысьвихремтрепе
щущихкрыльевповодьязавернутыепетлейсвисалипереднейлукияпокачивалась вседлекакмеш
окскрупойпридерживаялевойрукойлежавшеенаколеняхписьмоипытаясьразобратьпрыгающие
передглазамируныромашкапользовалась моимрасслабленнымсостояниемвсезамедляяизамедл
яяшагнадеясьчтояувлеченнаячтениемнезамечуеековарногоманевраидамейостановитьсяиспок
ойнопощипатьтравкутычегоэтоголубушкаанушевеликопытамиплутоватаякобылкаразочарова
нновсхрапнуладавайдавайхалтурщицаяустроилась поудобнейесливообщеможноустроитьсяпо
удобнейнатомпыточномпредметекоимявлялось дляменяжесткоеказенноеседлонатретийденьп
утиромашкинагриватоненькимиколечкамиспускалась допереднейлукизабиваясьмеждустрани
цамипухлогописьмакотороеядолжнабылавручитьповелителюдогевыикотороеужеминутпятьк
аксамовольновскрылаприпомощимагиинетронувувесистойпечатинаверевочкенааломвоскеот
четливопроступалоттискперстнятринадцатьруниперепле тающийсядракономединорогвцентр
етутмоизанятиялитературойдипломатиейигенеалогиейгрубопрервалиоченьгрубояедвауспела
подхватитьлисткипоползшиевразныестороныромашканеисправимаясаботажницазадумчивож
евалауздубряцаяжелезомвтовремякакнезнакомыйивесьмаподозрительныйтипобросшейнаруж
ностидемонстративнопотрясалпередлошадиноймордойсамодельнымарбалетомсгрязнойстрел
оймногоразовогоиспользованиятакчтонепонятнобылокогоонсобираетсяграбитьменяилирома
шкуяприподнялась настременахсинтересомрассматриваязаряжавленныйнаконечникянедумаюч
тоэтосамоеудачноеместодляторговлиантиквариатомдоверительносообщилаянезнакомцувотв
старминеувасбыегосрукамиоторваливернееотрубилизнаетелитамоченьнелюбятразбойниковр
омашкаобнюхалаарбалетпрезрительнофыркнулаинапрочьигнорируяграбителяпотянуласькап
петитнойзеленималинникаизвысокойгущикотороготолькочтовозниклоэточудовлаптяхпресту
пныйэлементзаметносмутилсянаконечникзатрепеталкакщенячийхвостикувыдораскаянияипо
каяниябылоещедалекозаблудшаяовцаупорствовалавогрехесребролюбияануткаживослезайско
нядевкаязыкатаякошелекилижизньдапошустрейслышишьяизобразилаусиленнуюработумысл
иладноубедилкошелекпахнулоозономлицограбителяпередернулось зрачкирасширились глазао
стекленелиионмедленноопустиварбалетотвязалибеспрекословноподалмнетощиймешокболта
вшийсяупоясаотмешкаразилокошкамиикуревомослабивверевкустягивавшуюгорловинуяпроп
устиласкозьпальцынесколькомелкихмонетмаловатодорогоймоймаловатосленцойработаешь
безогонькавпрочемтакужибытьвозьмувкачествеавансаосчастливилаяграбителяшвыряяемупо
дногипустоймешокипредупредилаячерезпаруднейэтойжедорогойназадпоедутакужбудьдобрп
остарайсяменянеразочароватьмужикнеотрываяотменязагипнотизированноговзглядамедленно
нагнулсяподнялмешокизастылстолбстолбомневсилахшевельнутьсябезмоеговедомакактолько
гореграбительскрылсяизвидуядеактивировалазаклинаниеипозволиларомашкеперейтисгалопа
налюбимуюеютрусцуписьмозажатоевовремяподсчетаденегуменямеждуколеняминемногопом
ялосьиутратилотоварныйвидвпрочемрассудилаяглавноенеоформлениеасодержаниеоноежеко
мпенсировалонедостаткирепейноголистаиспользованноговукромномместеагавотнаконециоб
омнепарастрокзадифирамбамизагадочномуарракктурупропустишьинезаметишьзавремяобуче

нияввысшейшколечародеевпифийитравницадептквавольхапроявиласебязнаюоченьплохонеуси
дчиванетерпеливасвоевольназнакомаяпеснялюбитзлыешуткиинеоднократнопереноситихсвос
питанниковнавоспитателейэтоонпроведрочтолидабылоодноведеркодовольнообъемистоестоя
лосебенабалкенаддверьюмоейкомнатыэдакийсамодельныйкапканнасоседейпошкольномуоб
щежитиюдабынеповаднобылобезспросуодалживатьуменяконспектыикастрюлиснавареннымн
анеделюборщомможетучительтакбынеразозлилсяеслибыведровсетакиопрокинулосьанеупало
емунаголовустоймявместесводойотличаетсяредкимиспособностямикпрактическойитеоретич
ескоймагиисильноразвитойинтуициейбыстроадаптируетсякнестандартнойситуациихаможетя
ещенебезнадежнанеприличнаякакаятограницаудогевыуэльфоввысокиетравыугномовскалыув
адлаковгрудывыброшеннойнаповерхностьземлиудриаддубыподметающиеоблакаудруидовка
менныекругиулюдейоблупленныестеныканалысзатхлойводойразделенныепаройтройкойподъ
емныхмостовдалысыестражникипринихбдительнодремлющиеупираясьнаржавыеалебардыазд
есьосиныиздевательствокакоетоособенноеслиучестьчтожителидогевывампирыхорошиетакие
осинысеребристыетрепещущиезаосинамищекочетнебоостроверхийеловыйковерсредикоторог
окоегдепроглядываютзатравленныеберезкиисосенкисамажедогевалежитвдолинекакплюшкан
аднерасписнойпиалыеслисмотретьсхолмакраяпиалывиденбелыйободокизосинвторойпотолщ
епотемнееизелейавцентреширокоезеленоедноскрапочкамисамадогевавкольцевозделанныхпо
лейиоблакахтуманаподойдешьвплотнуюкдеревьямнаставлялменяучительипошлешьмысленн
ыйсигналвглубьлесалюбойможешьдуматьочемугоднолишьбысформироватьмощнуютелепати
ческуюволнуакомумнееенаправитьнаобщейчастотектонибудьизстражейграницыуслышитясм
ущеннокашлянулалучшебыемуэтогонеслышатьнеобязательнопродумыватьочереднуюпакост
ьзнаюзнаютынанихсверхвсякоймерыгоразданонасейразпостарайсявоздержатьсяотоныхочемэ
тояхдаоволневампирыоченьвосприимчивыктелепатииисразуотреагируютнаееприсутствиехо
тяинесмогутдоскональнорасшифроватьтакчтонапирайнаколичествоаненакачествоваттакясмо
трюнадымящуюбанюнаморщивлоботусердияинамоюволнутутжереагируютпятьилишестьаде
птовкоторыеовеянныепаромвыбегаютиздверейивыпрыгиваютизоконатакованныевнезапноож
ившимивеникамирукибудущихколлегзанятышайкамиприкрывающимиотвениковсамоесокров
енноеучительусмиряетвеникиоднимдвижениембровиновзглядыадресованныешутниценедом
ытымиколлегаминесулятничегохорошегоясказалподуматьанетранслироватьзаклинанияжальч
тозагодыпроведенныевэтихстенахтытакиненаучиласькдуматьчтождумаюстоюподосинойнамо
рщивлобиромашкаужечтотожуетзеленаяслюнасочитсяизчерныхуголковбархатистыхгубразде
ленныхкольцамиудилтелепатироватьзначитсознательноделитьсямыслямискемнибудьдругим
делюсьпоследнимизлесатянетпрохладойсидящаянаветкеиволгаудивленнопокачиваетхвостом
вответнамоиумственныепотугилибозанятиеоказалосьмненепозубамлибоошарашенныестражи
границыпопадалинаместесраженныемоеймощнойдумоймоистаранияувенчалисьуспехоммину
тчерезсорокизаэтовремяяуспелапередуматьбольшечемзапредыдущиевосемнадцатьлетавотир
езультатагаподействовалоилионпроходилмимослучайноявпервыеувиделавампиравозможное
слибыонвозникизниоткудабылбледенкаксмертьинедвусмысленноскалилокровавленныезубыя
быегоиспугаласькаксобственноипланироваламоизнаниявобластивампироведениябазировалис
ьначеловеческихлегендахипреданияхотличавшихсяредкостнымпессимизмомктомужевсеграв
юрыкартиныгобеленынаскальнаяживописьизображаютвампировисключительноночьюивтем
нотекрыльязубыкогтивсеэтокажетсятакимстрашнымиогромнымтолькопотомучтотолкомниче
гонельзяразглядетьдневнойсветразвеялореолужасавпухипрахприсолнечномсветенафонебеск
райнихполейивысокихдеревьеввампирпоказалсямневозмутительномелкимибезобиднымправ
даяещенеспешиласьапришлосьмнегалантнопредложилирукувоспользоватьсякоторойвпрочем
янерискнулавампирулыбнулсяпоказавдлинныеклыкилюбойулыбнулсябыувидевкакясползлас
ъехалапокрутомуромашкиномубокуперекинувповодьячерезголовулошадиявыжидающеустав
иласьнавампиратражгранцыоказалсявышеменянаполголовыширокплечахивесьманедурен
собойдлинныетемныеволосыобрамлялиузкоезагорелоелицосложенныезаспинойкрыльяприда
валивампирунекотороесходствосмороемдемономпосланникомсмертидесятиаршиннаястатуяк

оторогоукрашалаактовыйзалвысшейшколычерныепронзительныечутьраскосыеглазавампира изучилимоюмалопривлекательнуювнешностьнотакинесумелиразгадатьчтозанейсокрыто

Висновок: при виконанні комп’ютерного практикуму було отримано навички частотного крипто аналізу. Здобуто навички роботи та аналізу потокових шифрів гамування адитивного типу на прикладі шифру Віженера. Закріплено раніше отримані знання.